

Práctica: JAAS contra un directorio LDAP

Objetivo: Implementar un Sistema de Autenticación y autorización que utilice como repositorio un directorio al que se accede mediante LDAP.

Desarrollo:

1. Crea una nueva instancia de ADAM (Active Directory Application Mode), como instancia única de nombre ATOS, crear una partición para nuestra aplicación que se llamara DC=ATOS, e importar el fichero de usuario.



Asistente para instalación de Active Directory Application Mode (ADAM)

Opciones de instalación
Se crea una instancia de ADAM cada vez que se instala ADAM.

Puede crear una instancia única, o puede instalar una réplica de una instancia existente.

Seleccione el tipo de instancia que desea instalar.

☒ Una instancia única
Esta opción crea automáticamente una nueva instancia de ADAM que usa las particiones de configuración y de esquema predeterminadas. La nueva instancia no podrá replicarse con las instancias existentes.

☐ Una réplica de una instancia existente
Esta opción crea una nueva instancia de ADAM que usa las particiones de configuración y de esquema replicadas desde otra instancia de ADAM. Puede también seleccionar las particiones de aplicación que desea replicar.

< Atrás Siguiente > Cancelar Ayuda

Asistente para instalación de Active Directory Application Mode (ADAM)

Nombre de instancia
El nombre de instancia se usa para diferenciar esta instancia de ADAM de otras instancias de ADAM en este equipo.

Escriba un nombre para esta instancia. El nombre debe reflejar el uso previsto para esta instancia de ADAM.

Nombre de instancia:

Ejemplo: Addressbook1

El nombre de servicio ADAM se crea cuando el nombre de instancia se combina con el nombre de producto. Se mostrará en la lista de los servicios de Windows.

Nombre de servicio ADAM:
ADAM_ATOS

< Atrás Siguiente > Cancelar Ayuda

Asistente para instalación de Active Directory Application Mode (ADAM)

Puertos
Los equipos se conectarán a esta instancia de ADAM usando puertos específicos en todas las direcciones IP asociadas con este equipo.

Los puertos mostrados a continuación son los primeros disponibles para este equipo. Para cambiar estos puertos, escriba los nuevos números de puerto en las cajas de texto debajo.

Si tiene pensado instalar Active Directory en este equipo, no use 389 para el puerto LDAP ni 636 para el puerto SSL, ya que Active Directory usa dichos números de puerto. Use los números de puerto disponibles del siguiente rango: 1025-65535.

Número de puerto LDAP:

Número de puerto SSL:

< Atrás Siguiente > Cancelar Ayuda

Asistente para instalación de Active Directory Application Mode (ADAM)

Partición de directorio de aplicaciones
Una partición de directorio de aplicaciones almacena datos específicos de la aplicación.

¿Desea crear una partición de directorio de aplicaciones para esta instancia de ADAM?

☐ No, no crear una partición de directorio de aplicaciones
Seleccione esta opción si la aplicación que planea instalar crea una partición de directorio de aplicaciones durante la instalación o si planea crear una más tarde.

☒ Sí, crear una partición de directorio de aplicaciones
Seleccione esta opción si la aplicación que desea instalar no crea una partición de directorio de aplicaciones después de ser instalada. Un nombre de partición válido es cualquier nombre completo que no existe en esta instancia. Un ejemplo de un nombre completo es CN=Partición1,DC=Woodgrove,DC=COM

Nombre de la partición:

< Atrás Siguiente > Cancelar Ayuda

Asistente para instalación de Active Directory Application Mode (ADAM)

Importación de archivos LDIF
Puede importar datos de archivos de Formato ligero de intercambio de directorios (LDIF) a su partición de directorio de aplicaciones de ADAM.

Para configurar el servicio ADAM de una forma determinada, importe uno o varios archivos LDIF mostrados a continuación.

☐ No importar archivos LDIF para esta instancia de ADAM

☒ Importar los archivos LDIF seleccionados para esta instancia de ADAM

Archivos disponibles:
MS-AZMan.LDF
MS-InetOrgPerson.LDF
MS-UserProxy.LDF

Archivos LDIF seleccionados:
MS-User.LDF

Agregar > < Quitar

< Atrás Siguiente > Cancelar Ayuda

Asistente para instalación de Active Directory Application Mode (ADAM)

Instalar ADAM
El Asistente para instalación de ADAM está instalando ADAM.

Instalando ADAM...

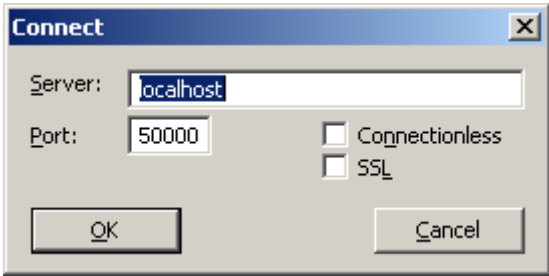
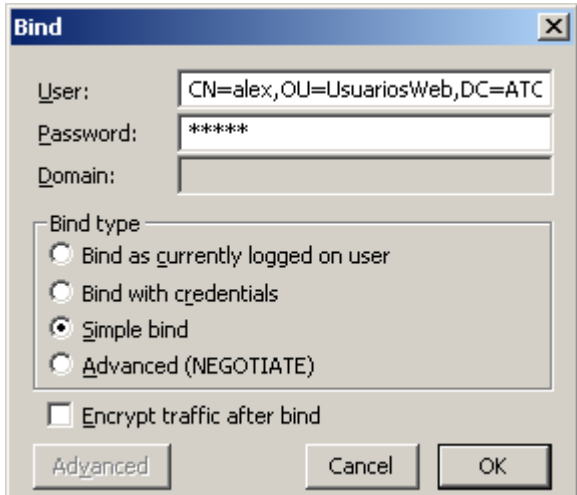
Espere mientras el asistente completa los siguientes pasos.

✓ Archivos copiados

Iniciando el servicio ADAM...

< Atrás Siguiente > Cancelar Ayuda

2. Con el editor ADSI conectar a localhost y el puerto indicado durante la instalación (50000), conectando con el nodo DC=ATOS
 - 2.1. Crear dos unidades organizativas, unas para usuario (UsuariosWeb) y otra para Roles (RolesWeb)
 - 2.2. Crear varios objetos de tipo *User*, con el CN (Common name) como el nombre del usuario, y estableciendo las contraseñas
 - 2.3. En la unidad organizativa RolesWeb crear un objeto de tipo *groupOfNames* cuyo CN sea el nombre del Role (Administrador y Usuario), en el atributo *member* añadir las cuentas de usuario ADAM, tal y como se ven en el DN (distinguishedName) de los usuarios creados, pe: *CN=alex,OU=UsuariosWeb,DC=ATOS*
 - 2.4. Añadir también en el grupo Readers de Roles los usuarios, para que puedan leer del directorio.
 - 2.5. Una vez configurado el directorio comprobamos si se hace login a través de la herramienta ldp.exe accesible desde el símbolo de sistemas de herramientas de ADAM.

<p>Conexión:</p>  <p>Authenticated as: 'CN=alex,OU=UsuariosWeb,DC=ATOS'.</p>	<p>Bind:</p> 
--	--

3. Creamos una nueva política en el fichero login.config.xml de la carpeta de configuración de JBOSS

```
<application-policy name="MiPolitica">
  <authentication>
    <login-module code="org.jboss.security.auth.spi.LdapLoginModule">
      <module-option name="java.naming.factory.initial">
        com.sun.jndi.Ldap.LdapCtxFactory
      </module-option>
      <module-option name="java.naming.provider.url">
        ldap://localhost:50000/
      </module-option>
      <module-option name="java.naming.security.authentication">
        simple
      </module-option>
      <module-option name="principalDNPrefix">
        cn=
      </module-option>
      <module-option name="principalDNSuffix">
        , ou=UsuariosWeb, dc=ATOS
      </module-option>
      <module-option name="rolesCtxDN">
        ou=RolesWeb, dc=ATOS
      </module-option>
      <module-option name="uidAttributeID">member</module-option>
      <module-option name="matchOnUserDN">true</module-option>
      <module-option name="allowEmptyPasswords">false</module-option>
      <module-option name="roleAttributeID">cn</module-option>
      <module-option name="roleAttributeIsDN">false</module-option>
      <module-option name="allowEmptyPasswords" value="false"/>
    </login-module>
  </authentication>
</application-policy>
```

3.1. Recordad que si cambiáis el nombre de la política hay que cambiar el fichero jboss-web.xml de la aplicación Web.

4. Comprobar el funcionamiento de la aplicación Web